(12) UK Patent Application (19) GB (11) 2 246 457 (13) A

(43) Date of A publication 29.01.1992

(21) Application No 9016364.3

(22) Date of filing 25.07.1990

(51) INT CL[5]
G06F 12/14

(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
EP 0262025 A2 EP 0192243 A2

(58) Field of search
UK CL (Edition K) G4A AAP
INT CL[5] G06F 1/00 12/14
Online database: WPI

(71) Applicant
Bluetron Limited

(Incorporated in Ireland)

2 Leeson Park, Ranelagh, Dublin 6, Ireland

(72) Inventor
James Martin Sheeran

(74) Agent and/or Address for Service
Marks & Clerk
57-60 Lincoln's Inn Fields, London, WC2A 3LS,
United Kingdom

(54) Controlling access to stored data

(57) A security circuit 2 for controlling access to data stored in a read/write memory circuit 7 and a fixed disk 8 of a computerised device 1 includes a comparator 20 which carries out various comparison operations regarding user names, passwords and permitted access times. A counter register 23 is used to limit the number of attempts the user may make at accessing stored data and a disabling circuit 24 is operative to disable a printer controller 10, a video controller 12 and a keyboard encoder 4. A memory blocking circuit 22 is arranged to control access of a microprocessor control unit 5 to stored data according to a security level for each user. Thus, users may have partial access to stored data and versatility is achieved.

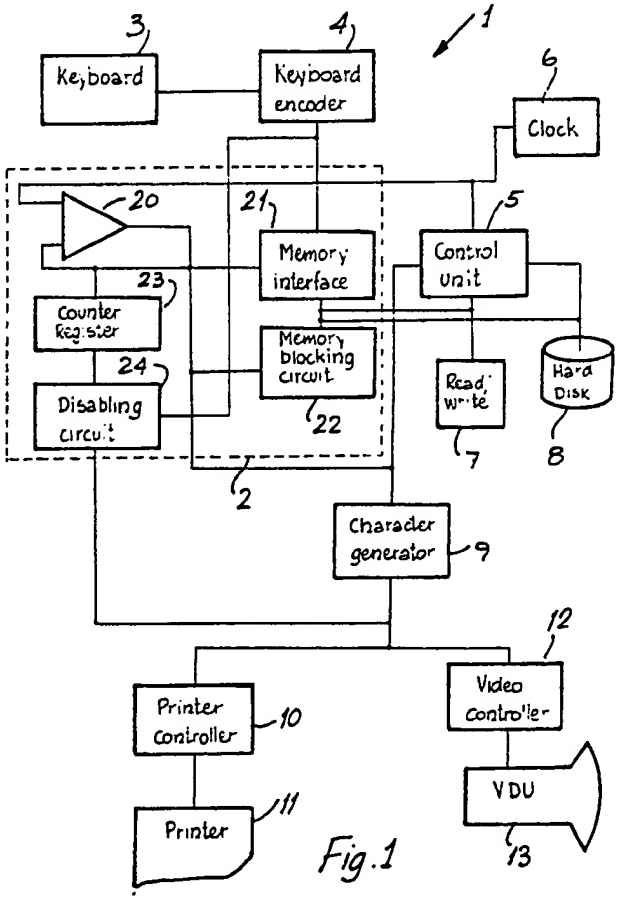

Fig.1

BEST AVAILABLE COPY

GB 2 246 457 A

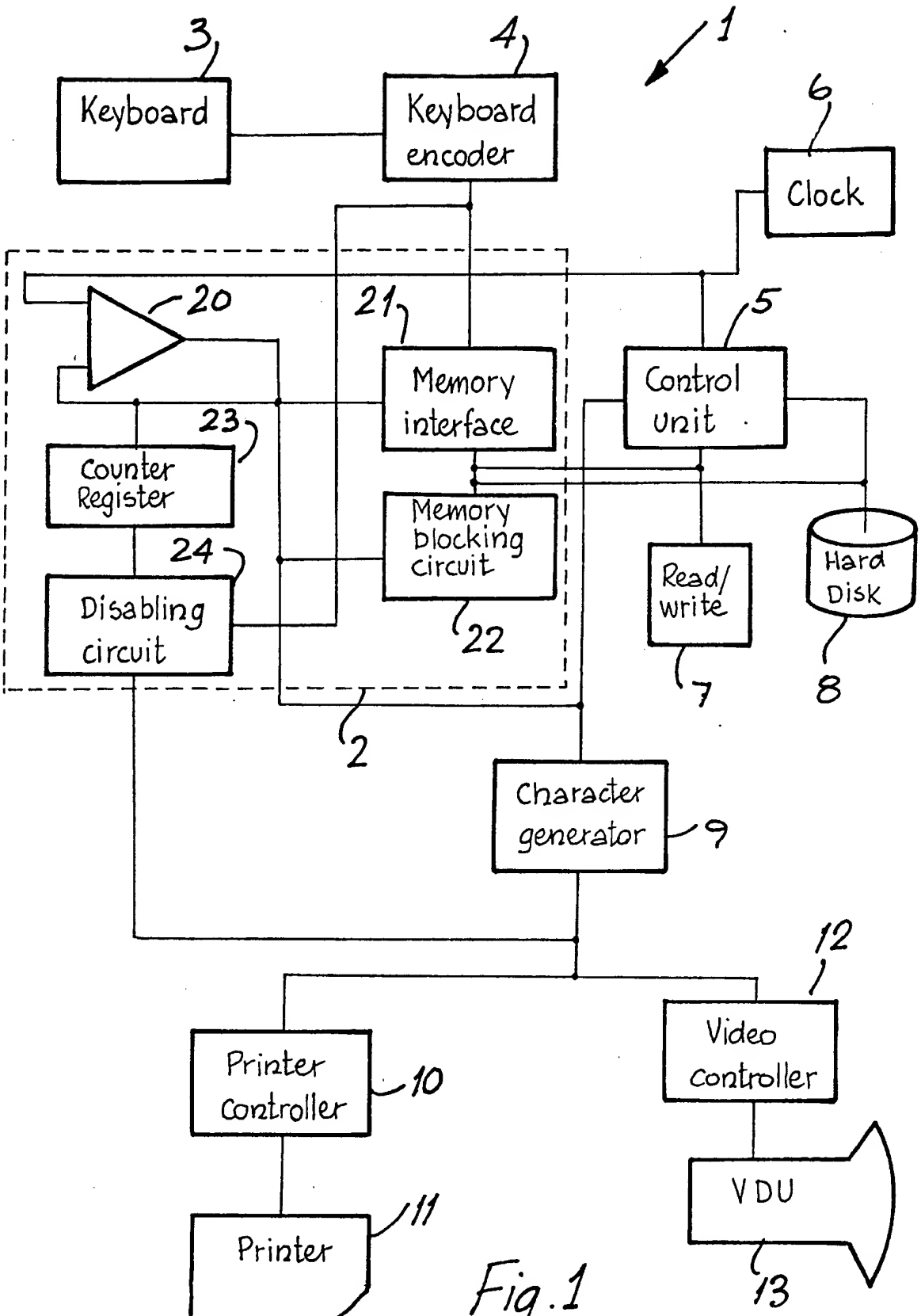
1
3
Keyboard
4
Keyboard encoder
6
Clock
20
21
5
Memory interface
Control unit
23
Counter Register
Memory blocking circuit
24
Disabling circuit
22
Read/ write
Hard Disk
7
8
2
Character generator
9
12
Video controller
Printer Controller
10
VDU
11
Printer
13

Fig. 1

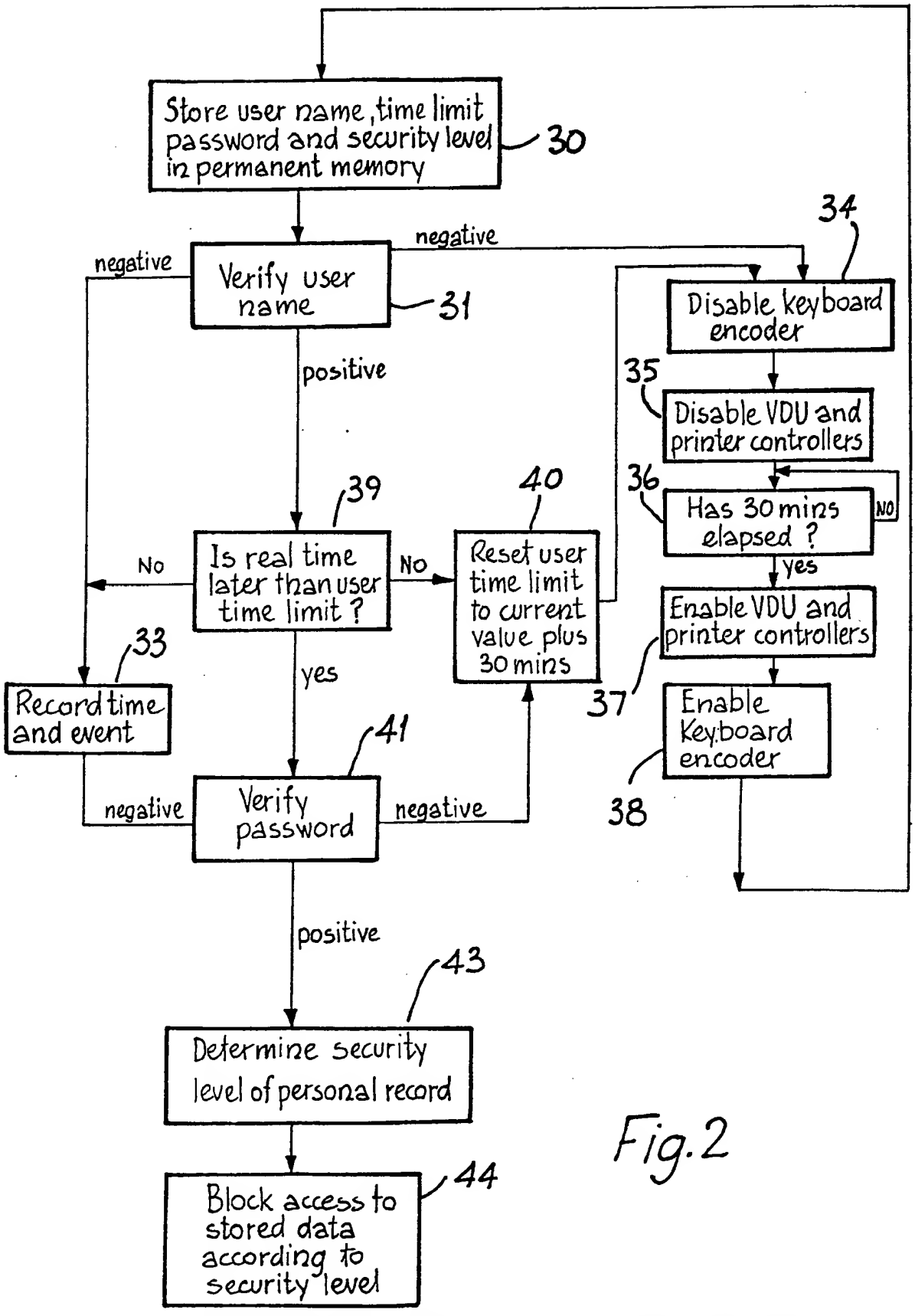
Store user name, time limit password and security level in permanent memory
30
Verify user name
31
negative
positive
34
Disable keyboard encoder
35
Disable VDU and printer controllers
36
Has 30 mins elapsed ?
NO
yes
Enable VDU and printer controllers
37
Enable Keyboard encoder
38
39
Is real time later than user time limit ?
No
No
40
Reset user time limit to current value plus 30 mins
33
Record time and event
yes
41
Verify password
negative
negative
positive
43
Determine security level of personal record
44
Block access to stored data according to security level

Fig. 2

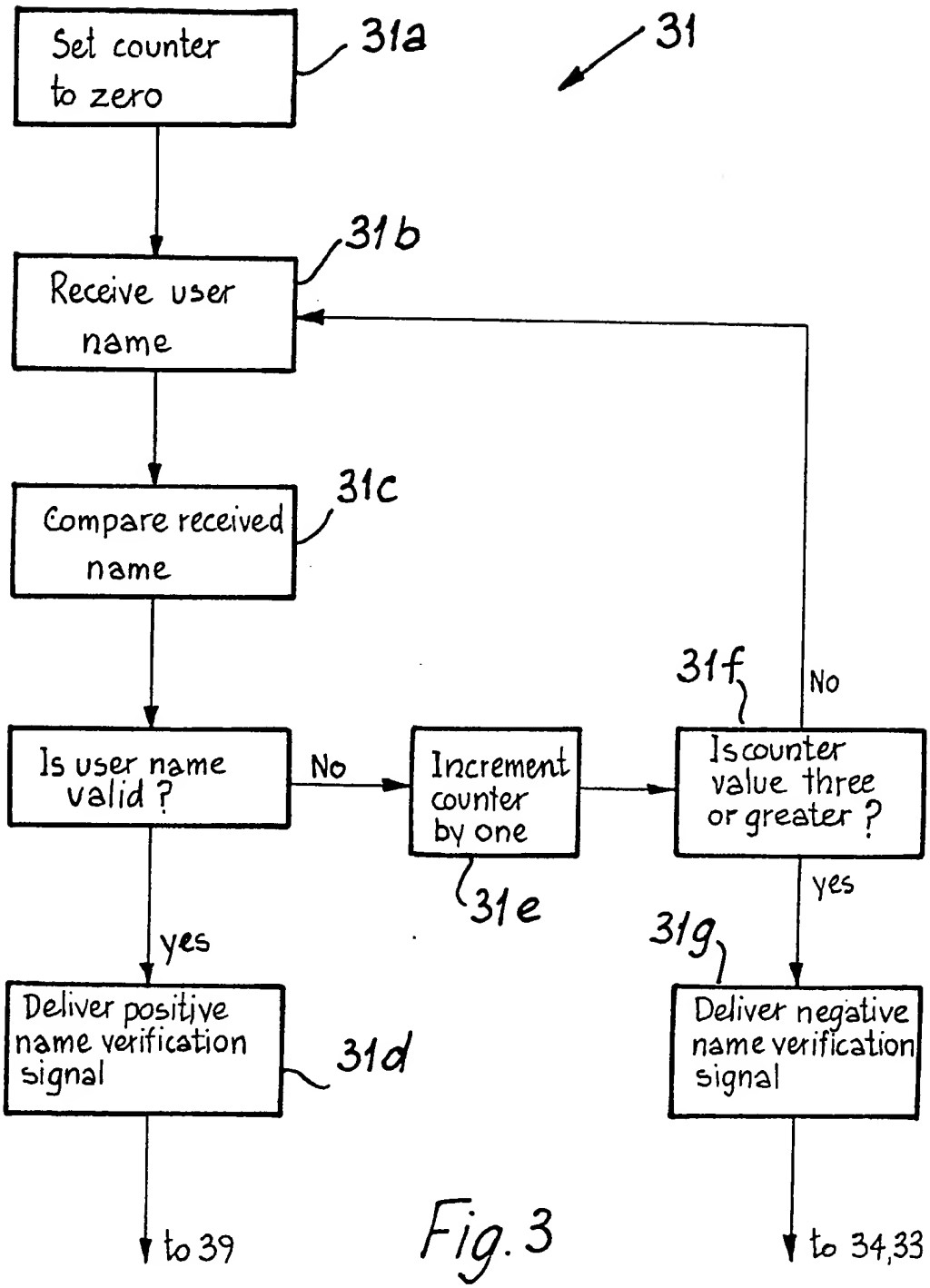
Set counter to zero
31a
31
31b
Receive user name
31c
Compare received name
Is user name valid ?
No
Increment counter by one
31e
31f
No
Is counter value three or greater ?
yes
yes
31g
Deliver positive name verification signal
31d
Deliver negative name verification signal
to 39
to 34,33

Fig. 3

"Control of access to data stored in a storage medium"

The present invention relates to the control of access to data stored in a storage medium in a computerised device.

The control of access to data in a storage medium is particularly important where scientific test data, confidential document text or other data which should not be made available to unauthorised people is stored. Security circuits have been devised to control access to such data and these circuits are generally operational either to prevent a person utilising any processing circuits or to allow a person access to all of the facilities. They thus allow little versatility in use of the circuits and further, if an unauthorised person succeeds in by-passing the security circuit, he or she has unrestricted access to all data.

The present invention is directed towards providing an improved security circuit and method to overcome these problems.

According to the invention, there is provided a security circuit for controlling access to data stored in a storage

medium in a data storage and processing apparatus comprising an input device, an input device encoder, a control circuit, a real time clock, an output device controller, and an output device, in which said storage medium comprises a permanent memory device and a read/write memory circuit, the security circuit comprising:-

a memory interface for directing storage in the permanent memory device of a personal record for each user authorised to access stored data, the personal record including a name, a password, a security level indication, and a time limit after which the respective user is allowed access to stored data;

a comparator for verifying a name received at the input device by comparing the received name with the stored name in the personal record and for directing delivery of a name verification signal to the output device and to the permanent memory device;

a disabling circuit for disabling the input device encoder and the output device controller if the name verification signal is negative;

means at the comparator for comparing time of the real time clock with the time limit in the

respective personal record and for directing delivery of a time verification signal to the output device and to the permanent storage device for storage in the personal record if the name verification signal is positive;

means at the memory interface circuit for re-setting the time limit to a value which is a pre-determined amount later than the current value, and for subsequently directing disabling of the input device encoder and of the output device controller if the time verification signal is negative;

means at the comparator for verifying a password received at the input device by comparing the received password with the stored password of the respective personal record and for delivering a password verification signal to the output device and to the permanent storage device for storage in the respective personal record if the time verification signal is positive;

means at the disabling circuit for disabling the input device encoder and the output device controller if the password verification signal is negative;

a memory blocking circuit for retrieving the security level indication from the respective personal record and delivering a memory blocking signal to the control unit to facilitate setting of storage areas in the permanent memory device and in the read/write memory circuit from which the control unit may not read data if the password verification signal is positive.

According to another aspect, the invention provides a method of controlling access to data stored in a storage medium in a data storage and processing apparatus comprising an input device, an input device encoder, a control circuit, a real time clock, an output device controller, and an output device, in which said storage medium comprises a permanent memory device and a read/write memory device, the method comprising the steps of:-

directing storage in the permanent memory device of a personal record for each user authorised to access stored data, the personal record including a name, a password, a security level indication, and a time limit after which the respective user is allowed access to stored data;

verifying a name received at the input device by comparing the received name with the stored name in

the personal record and directing delivery of a name verification signal to the output device and to the permanent memory device for storage in the personal record;

disabling the input device encoder and the output device controller if the name verification signal is negative;

comparing time of the real time clock with the time limit in the respective personal record and directing delivery of a time verification signal to the output device and to the permanent storage device for storage in the personal record if the name verification signal is positive;

re-setting the time limit to a value which is a pre-determined amount later than the current value, and subsequently directing disabling of the input device encoder and of the output device controller if the time verification signal is negative;

verifying a password received at the input device by comparing the received password with the stored password of the respective personal record and delivering a password verification signal to the output device and to the permanent storage device

for storage in the respective personal record if the time verification signal is positive;

disabling the input device encoder and the output device controller if the password verification signal is negative;

retrieving the security level indication from the respective personal record and delivering a memory blocking signal to the control unit to facilitate setting of storage areas in the permanent memory device and in the read/write memory circuit from which the control unit may not read data if the password verification signal is positive.

In one embodiment, the method comprises the further steps of initially setting a counter register to zero, incrementing the counter register after comparing the password or name, and repeating said comparison and incrementing operations a pre-set number of times according to the counter register.

The invention will be more clearly understood from the following description of some preferred embodiments thereof, given by way of example only with reference to the accompanying drawings in which:-

Fig. 1 is a schematic representation of a computerised device incorporating a security circuit of the invention; and

Figs. 2 and 3 are flow diagrams illustrating operation of the security circuit.

Referring to the drawings, and initially to Fig. 1, there is illustrated a computerised device 1 incorporating a security circuit 2 of the invention. The security circuit 2 is indicated by interrupted lines. The computerised device 1 comprises a keyboard 3 connected to a keyboard encoder 4 which provides a 7-bit representation for each key of the keyboard 3. The computerised device 1 also includes a microprocessor control unit 5 and a real-time clock 6 having a battery backup. A storage medium for the computerised device 1 comprises a read/write memory circuit 7 and a fixed disk 8. For output of processed data and of data stored in the read/write memory circuit 7 and the fixed disk 8, the device 1 includes a character generator 9 connected to a printer controller 10 for a printer 11 and to a video controller 12 for a visual display unit (VDU) 13.

The security circuit 2 comprises a comparator 20 having an input connected to the keyboard encoder 4, the clock 6 and to various other portions of the computerised device 1 via a memory interface 21. The memory interface 21 is connected to

a memory blocking circuit 22 and the security circuit 2 also includes a counter register 23 and a disabling circuit 24. The disabling circuit 24 is connected to the video controller 12 and the printer controller 10.

The computerised device 1 is arranged to carry out processing of data received at the keyboard 3 and stored in the fixed disk 8 and in the read/write memory circuit 7.

Referring to Figs. 2 and 3, in step 30, the memory interface 21 of the security circuit 2 initially directs storage in the fixed disk 8 of a personal record for each user authorised to access the stored data. Typically, the memory interface 21 is operated by a supervisor and the personal record includes a name for each authorised user, a password, a security level and a time limit. There are five security levels in this case numbered 1 through 5, with the lower numbers allowing access to a lesser amount of data than the higher numbers. The time limit is a time before which a user is not allowed access to stored data. For example, if the time limit is 15.00 a user may not access stored data before 15.00 each day. The personal record is stored in the fixed disk 8 and is thus not lost when the computerised device 1 is switched off.

When a user wishes to access stored data, in step 31 he or she keys in a name at the keyboard 3. The comparator 22 retrieves the received name from the keyboard encoder 4 and compares

this with all of the stored names in the fixed disk 8. This is indicated in greater detail in Fig. 3. Initially, the counter register 23 is set to zero in step 31(a) and the user name is received at the keyboard 3 in step 31(b). In step 31(c) the comparator 20 compares the received user name with the stored names in the fixed disk 8 and in step 31(d) delivers a positive name verification signal to the VDU 13 and/or the printer 11 if the name is located. If the name has not been found in the fixed disk 8, the counter register 23 is incremented by 1 in step 31(e). In step 31(f) a check is made as to the value of the counter register and if the value is less than 3, the user is prompted to input a user name again and the procedure is repeated until three names have been inputted. If after repetition of the procedure three times, a name has not been located in the hard disk 8, in step 31(g) the comparator 20 delivers a negative name verification signal to either the printer 11 and/or the VDU 13.

In step 33, the comparator 20 directs recording of the time and the fact that the verification has been negative in the hard disk 8. In step 34 the disabling circuit 24 disables the keyboard encoder 4 and in step 35 the VDU and printer controllers 10 and 12 are disabled. In step 36 the disabling circuit 24 monitors real time after disabling of the VDU and printer controllers 10 and 12 and the keyboard encoder 4 and after 30 minutes has elapsed it enables the VDU and printer controllers in step 37 and enables the keyboard encoder in

step 38. When this has been done, the procedure may start again.

On the other hand, if the comparator 20 locates the user name on the fixed disk 8, a positive verification signal is outputted at the printer 11 and/or the VDU 13 and in step 39 the comparator 20 compares real time with the recorded user time limit for the personal record associated with the located name. If real time is earlier than the time limit a negative time verification signal is output at the printer 11 and/or the VDU 14 and in step 40 the memory interface 21 directs re-setting of the time limit to the current value plus 30 minutes and the procedure of steps 34 through step 38 is repeated. The event is stored in the hard disk 8 in step 33. If real time is later than the time limit, a positive time verification signal is delivered and in step 41 a user password is received at the keyboard 3 and is compared with the stored password of the personal record in a similar manner to the procedure for verifying a received user name illustrated in Fig. 3. The only difference being that the comparator 20 only checks in the single personal record and not in all of the personal records as it does when a name is received. If the password is not verified the fact is recorded in step 33 and the procedure of steps 40 and 34 through 38 is repeated. Further, a negative password verification signal is output at the printer 11 and/or the VDU 13.

In step 43, the memory interface 21 retrieves the security level stored in the personal record and in step 44 the memory blocking circuit blocks access to the read/write memory circuit 7 and to the fixed disk 8 according to the security level by transmitting an appropriate signal to the control unit 5. For example, if the security level is "5", a user is allowed access to all of the data stored on the fixed disk 8, however, if the security level is 2 then only a pre-set portion of the fixed disk 8 may be accessed. The memory blocking circuit 22 carries out this function by instructing the control unit 5 to block the relevant addresses on the memory.

It will thus be appreciated that a user is allowed access to stored data according to the criterion of a name, a password and a time limit. Further, access of certain address locations is blocked according to a security level. It is envisaged that it will be extremely difficult for a person to circumvent the security circuit 2 as the keyboard encoder is disabled and it is impossible to direct instructions of the keyboard 3 into the microprocessor control unit 5. Further, because the VDU and printer controllers are disabled, the user does not receive any output. By re-setting the personal record time limit to 30 minutes later than the current value, the user is in the same position more than half an hour later when the VDU and printer controllers and the keyboard encoder

have been enabled again. Because of operation of the memory blocking circuit 22, the supervisor is given versatility in deciding on access of users to stored data and thus the one computerised device may be used by several different people, each having their own personal restrictions as to access to stored data. At any stage, the supervisor may obtain a print-out at the printer 11 of all security events over a time period, which information is retrieved from the hard disk 8.

The invention is not limited to the embodiments hereinbefore described but may be varied in construction and detail.

CLAIMS

1. A security circuit for controlling access to data stored in a storage medium in a data storage and processing apparatus comprising an input device, an input device encoder, a control circuit, a real time clock, an output device controller, and an output device, in which said storage medium comprises a permanent memory device and a read/write memory circuit, the security circuit comprising:-

a memory interface for directing storage in the permanent memory device of a personal record for each user authorised to access stored data, the personal record including a name, a password, a security level indication, and a time limit after which the respective user is allowed access to stored data;

a comparator for verifying a name received at the input device by comparing the received name with the stored name in the personal record and for directing delivery of a name verification signal to the output device and to the permanent memory device;

a disabling circuit for disabling the input device encoder and the output device controller if the name verification signal is negative;

means at the comparator for comparing time of the real time clock with the time limit in the respective personal record and for directing delivery of a time verification signal to the output device and to the permanent storage device for storage in the personal record if the name verification signal is positive;

means at the memory interface circuit for re-setting the time limit to a value which is a pre-determined amount later than the current value, and for subsequently directing disabling of the input device encoder and of the output device controller if the time verification signal is negative;

means at the comparator for verifying a password received at the input device by comparing the received password with the stored password of the respective personal record and for delivering a password verification signal to the output device and to the permanent storage device for storage in the respective personal record if the time verification signal is positive;

means at the disabling circuit for disabling the input device encoder and the output device controller if the password verification signal is negative;

a memory blocking circuit for retrieving the security level indication from the respective personal record and delivering a memory blocking signal to the control unit to facilitate setting of storage areas in the permanent memory device and in the read/write memory circuit from which the control unit may not read data if the password verification signal is positive.

2. A security circuit as claimed in claim 1, further comprising a counter register and in which the comparator comprises means for initially setting the counter register to zero, for incrementing the counter register after comparing the password or name, and for repeating said comparison and incrementing operations a pre-set number of times according to the counter register.

3. A method of controlling access to data stored in a storage medium in a data storage and processing apparatus comprising an input device, an input device encoder, a control circuit, a real time clock, an output device

controller, and an output device, in which said storage medium comprises a permanent memory device and a read/write memory device, the method comprising the steps of:-

directing storage in the permanent memory device of a personal record for each user authorised to access stored data, the personal record including a name, a password, a security level indication, and a time limit after which the respective user is allowed access to stored data;

verifying a name received at the input device by comparing the received name with the stored name in the personal record and directing delivery of a name verification signal to the output device and to the permanent memory device for storage in the personal record;

disabling the input device encoder and the output device controller if the name verification signal is negative;

comparing time of the real time clock with the time limit in the respective personal record and directing delivery of a time verification signal to the output device and to the permanent storage

device for storage in the personal record if the name verification signal is positive;

re-setting the time limit to a value which is a pre-determined amount later than the current value, and subsequently directing disabling of the input device encoder and of the output device controller if the time verification signal is negative;

verifying a password received at the input device by comparing the received password with the stored password of the respective personal record and delivering a password verification signal to the output device and to the permanent storage device for storage in the respective personal record if the time verification signal is positive;

disabling the input device encoder and the output device controller if the password verification signal is negative;

retrieving the security level indication from the respective personal record and delivering a memory blocking signal to the control unit to facilitate setting of storage areas in the permanent memory device and in the read/write memory circuit from

which the control unit may not read data if the password verification signal is positive.

4. A method as claimed in claim 3, comprising the further steps of initially setting a counter register to zero, incrementing the counter register after comparing the password or name, and repeating said comparison and incrementing operations a pre-set number of times according to the counter register.

5. A security circuit substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawings.

6. A method substantially as hereinbefore described with reference to, and as illustrated in the accompanying drawings.

This Page is inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox